Nos. 22-55988, 22-56036

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AL OTRO LADO, INC., *et al.*,
Plaintiffs-Appellees/ Cross Appellants,

v.

ALEJANDRO MAYORKAS, Secretary of Homeland Security, *et al.*,
Defendants-Appellants/ Cross-Appellees,
and
the EXECUTIVE OFFICE FOR IMMIGRATION REVIEW,
Appellant/Cross-Appellee.

On Appeal from a Final Judgment of the U.S. District Court for the Southern District of California (Civil Action No. 17-cv-02366-BAS-KSC)

THE GOVERNMENT'S MOTION TO CONTINUE THE SEAL ON PORTIONS OF SUPPLEMENTAL EXCERPTS OF RECORD, VOLUMES 3-4 (Dkt. No. 29)

BRIAN M BOYNTON
Principal Deputy
Assistant Attorney General
Civil Division

WILLIAM C. PEACHEY
Director

ALEXANDER J. HALASKA
Senior Litigation Counsel

KATHERINE J. SHINNERS
Senior Litigation Counsel
U.S. Department of Justice Civil Division
Office of Immigration Litigation
District Court Section
P.O. Box 868, Ben Franklin Station
Washington, D.C. 20044
Tel: (202) 598-8259
katherine.j.shinners@usdoj.gov
JASON WISECUP
Trial Attorney

Counsel for the Government

INTRODUCTION

Appellants/Cross-Appellees (the government) respectfully move this Court to continue the seal on certain portions of Appellees/Cross-Appellants' (Appellees or Plaintiffs) Supplemental Excerpts of Record, Volumes 3 and 4 (Dkt. No. 29) ("SER" Volumes 3-4) accompanying their Second Brief on Cross Appeal, which were provisionally filed under seal pursuant to Circuit Rule 27-13(f).[1]

The documents at issue relate to the operation of land ports of entry along the U.S.-Mexico border. There are compelling reasons to keep portions of these documents sealed because they contain sensitive law enforcement information that, if made public, may seriously compromise those operations and thus compromise border and national security. Some of these documents additionally reveal internal government deliberations, disclosure of which would have a chilling effect on agency decisionmaking. There are also compelling privacy and security reasons to continue the seal on those portions of the documents that contain email addresses and phone numbers of U.S. government employees and identifying information of subjects of and witnesses to law enforcement and internal investigations, such as witnesses in an Office of Inspector General ("OIG") investigation. Additionally, this sensitive information has little to no bearing on the issues on appeal.

Appellees stated that they take no position on this motion.

[1] The government does not seek to continue the seal on Appellees' Second Brief on Cross Appeal.

PROCEDURAL BACKGROUND

This case centers on CBP's now-superseded metering practices at land ports of entry along the U.S.-Mexico border. *See* Opening Brief (Dkt. No. 12). When a port of entry was metering, a CBP officer generally stood at the international boundary line between the United States and Mexico and preliminarily screened pedestrians' travel documents. Travelers who presented what appeared to be facially sufficient entry documents were permitted to cross the border and proceed to a primary inspection booth inside the port of entry to be processed. Noncitizens without such documents may have been instructed to wait to cross the border until the port had sufficient capacity—including personnel and holding space, and taking into account CBP's and OFO's many other statutory responsibilities, *see* 6 U.S.C. §§ 211(c), 211(g)—to process their resource-intensive applications for admission and hold them pending transfer out of CBP custody. The district court below determined that metering practices were unlawful regardless of their justification, based on its interpretation of the relevant statutes as applying to noncitizens who were still in Mexico and requiring their inspection and referral for asylum processing as applicable. 1-ER-96–117. The district court did not, therefore, address Appellees' argument that justifications for metering were pretextual. 1-ER-117. The district court granted summary judgment for the government on Appellees' claims under the Immigration and Nationality Act and Alien Tort Statute. 1-ER-127–128. This cross-appeal followed.

On February 21, 2022, Appellees filed their Second Brief on Cross Appeal and Volumes 3 and 4 of their Supplemental Excerpts of Record provisionally under seal. *See* Dkt Nos. 23, 29. The government moves to continue the seal in this Court on the following portions of their Supplemental Excerpts of Record Volumes 3-4 (SER Volumes 3-4) that were filed under seal in the district court:

SER Volume 3

1. Portions of Exhibit 22 (Office of Inspector General Memorandum and Exhibits) to Plaintiffs' Reply in Support of Their Motion for Summary Judgment (3-SER-519–534) that contain names of witnesses and investigators and employee contact information;

2. Portions of Exhibit 38 (Leutert Merits Expert Report) to Plaintiffs' Reply in Support of Their Motion for Summary Judgment in Support of Their Motion for Summary Judgment (3-SER-535–550) that contain employee contact information, information about the distance between the international boundary line and the location at which officers staffed the limit line position, and a whistleblower name;

3. Portions of Exhibit 4 (Howe Deposition) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (3-SER-569–596), which contains information related to the Laredo Field Office Mass Migration Contingency Plan;

4. Portions of Exhibit 8 (Office of Professional Responsibility Investigation) to

Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (3-SER-600–38) that contain employee and witness names and contact information, and a "muster" involving sensitive details of CBP operations;

5. Portions of Exhibit 17 (Marin Deposition) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (3-SER-684–723) that contain information related to mass migration contingency plans;

SER Volume 4

6. Portions of Exhibit 29 (March 2016 Email Communications) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-812–815) that contain portions of the overflow contingency plan involving staffing contingencies and employee contact information;

7. Portions of Exhibit 38 (May 2016 Email Communications) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-816–19) that contain employee contact information;

8. The entirety of Exhibit 54 (October 2016 Email Communications) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-821–823), which contains internal deliberations regarding policy, details of contingency planning, and employee information;

9. Portions of Exhibit 83 (April 2018 Metering Memorandum) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary

Judgment (4-SER-846–48) that contain an employee's phone number;

10. The entirety of Exhibit 89 (April 2018 Email Communication) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-849–62), which contains communications with the Mexican government and law enforcement techniques and sources;

11. Portions of Exhibit 105 (August 2018 Email Communication) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-895–97) that contain employee contact information;

12. Portions of Exhibit 109 (November 2018 Email Communication) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-898–902) that contain employee contact information and internal agency deliberations;

13. Portions of Exhibit 110 (November 2018 Email Communication) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-903–06) that contain employee contact information and deliberative information;

14. Portions of Exhibit 111 (November 2018 Email Information) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-907–12) that contain employee contact information and deliberative information;

15. Portions of Exhibit 112 (August 2018 Email Communication) to Plaintiffs' Memorandum of Points and Authorities in Support of Their Motion for Summary Judgment (4-SER-913–16) that contain employee emails and phone numbers.

The government attaches hereto redacted versions of SER Volumes 3 and 4 in which the portions of the documents containing the sensitive material described above are redacted. *See* Exhibits A & B.

ARGUMENT

Although there is "a strong presumption in favor of access to court records," a party seeking to seal judicial records can "overcom[e] this strong presumption by meeting the 'compelling reasons' standard." *Ctr. for Auto Safety v. Chrysler Group LLC*, 809 F.3d 1092, 1096 (9th Cir. 2016). Compelling reasons include "when [] 'court files might [] become a vehicle for improper purposes,' such as the use of records to gratify private spite, promote public scandal, circulate libelous statements, or release trade secrets." *Kamakana v. City & Cty. of Honolulu*, 447 F.3d 1172, 1179 (9th Cir. 2006).

Here, there are compelling reasons to seal the information about port operations, contingency plans, communications with the government of Mexico, deliberative agency materials, and other law-enforcement sensitive information contained in SER Volumes 3-4. As the attached declarations establish, the security of the southwest border can be severely compromised if these details about the

operations of U.S. ports are widely publicly disclosed because they expose ports' vulnerabilities, and anyone or any entity would have access to information about the workings, resources, and division of resources along the border. *See Washington v. U.S. Dep't of State*, 318 F. Supp. 3d 1247, 1261 (W.D. Wash. 2018) (the State Department proved irreparable injury by showing harm in disclosing technical data relating to reproducing weapons). Other sensitive information includes communications with the government of Mexico, including sensitive intelligence relating to joint efforts to maintain border security, the release of which would not only chill cross-border security efforts but would also similarly expose the ports' vulnerabilities. Release of such information compromises the ports' operations and exposes ports to higher risk of criminal activity—such as drug and weapons trafficking—which in turn threatens the public health and safety of the United States. Irreparable injury is thus likely to ensue absent sealing.

There are also compelling reasons to seal internal agency deliberations relating to non-final decisions or actions. Disclosure of such deliberative material would have a chilling effect on agency decisionmaking. *Scalia v. Int'l Longshore & Warehouse Union*, 336 F.R.D. 603, 610 (N.D. Cal. 2020) (quoting *N. L. R. B. v. Sears, Roebuck & Co.*, 421 U.S. 132, 150 (1975) ("The underlying premise of the [deliberative process] privilege is that agency decision-making might be impaired if discussions within the agency were subject to public review, thereby discouraging 'frank

discussion of legal or policy matters.").

Additionally, the Court should permit the government to keep under seal the identifying information of whistleblowers and witnesses to the OIG investigations and of employees with sensitive positions, as well as employee email addresses and other contact information that is contained throughout SER Volumes 3-4, the disclosure of which would raise genuine security concerns for those employees as well as for the agency. Irreparable injury is thus likely to ensue absent sealing.

A. Compelling Security Reasons Favor Continuing the Seal on Documents Containing Detailed Operational and Law Enforcement Information That Exposes CBP's Potential Vulnerabilities.

The Court should continue the seal on sensitive details about CBP's operations along the U.S.-Mexico border. The public release of this law-enforcement information would harm CBP's operations and impair cross-border security, for the reasons stated in the September 4, 2020 Declaration of Vernon Foret, former Executive Director for Operations, Office of Field Operations (OFO) ("Foret Decl."), attached hereto as Exhibit C, and the March 9, 2020 Declaration of Mr. Foret ("Second Foret Dec."), attached hereto as Exhibit D. As the district court recognized, compelling reasons exist to permit "targeted redactions" of detailed information about the infrastructure and operations of specific ports of entry, including contingency planning, and communications with, or information shared by, the Government of Mexico regarding border-related issues. *See Al Otro Lado v. Mayorkas*, No. 17-cv-2366, ECF No. 510, 2020 WL 4551687, at *5, 6, 7, 9-11, (S.D.

Cal. Aug. 6, 2020).

Port-Specific Processing and Contingency Planning. First, the Court should continue the seal on specific information about contingency planning and port infrastructure and resources, contained throughout SER Volumes 3-4. *See* 3-SER-535–50 (Ex. 38, Leutert Merits Expert Report); 3-SER-569–96 (Ex. 4, Howe Deposition); 3-SER-684–723 (Ex. 17, Marin Deposition); 4-SER-535–550 (Ex. 38, Email Communications); 4-SER-812–15 (Ex. 29, Email Communications); 4-SER-816–19 (Ex. 38, Email Communications); 4-SER-821–23 (Ex. 54, Email Communications).

Sealing is warranted because these documents provide detailed information, for specific ports of entry, CBP, and DHS, that, if known, could allow bad actors to exploit operational vulnerabilities. *See* Foret Decl. ¶¶ 16-20 (discussing risks of disclosure of San Ysidro contingency plan and other similar contingency plans). These documents constitute or contain operational plans and actions to address migration events and surges, and reveal specific operational and infrastructure details, specific operational steps, and the specific decision points for an agency to take particular actions. *See* Foret Decl. ¶¶ 16-17. Contingency plans provide "detailed snapshot[s] of the operational environment," and provide insight into "how the agency may assess a similar migration surge in the future, and thus provide[] hostile actors with a roadmap for how to potentially interfere in such a response."

Foret Decl. ¶ 17.[2] The Court should seal this information to protect against such harms.

Other documents contain similarly sensitive information relating to planning for migration events. For example, emails relating to CBP's decision to open a particular processing facility (*see* 4-SER-820–23) would reveal both resource limitations as well as information obtained from foreign partners. Second Foret Decl. ¶¶ 11–12. As explained in the Second Foret Declaration, and as held by the district court, this information should be kept confidential to avoid divulging operational vulnerabilities. *See Al Otro Lado, Inc. v. Wolf*, 2020 WL 4551687, at *6 (S.D. Cal. Aug. 6, 2020) (citing Second Foret Decl. ¶ 11).

These documents also contain sensitive information about officers' physical placement at the Ports (*see* 3-SER-543–44), which could be exploited by individuals seeking to evade law enforcement. *See* Foret Decl. ¶¶ 21-22.

For these compelling reasons, the Court should continue the seal on the portions of SER Volumes 3-4 that contain this information, as set forth in the proposed redactions attached at Exhibits A and B.

Communications and Information-Sharing with the Government of Mexico. The Court should also continue the seal on the portions of SER Volumes 3-4

[2] CBP states that it has a continued need to have contingency plans and be able to implement such plans in the future, and that there are elements of these plans that do not change significantly over time and that may be relied upon again in the future.

that reflect the U.S. government's communications with Mexico about topics concerning and impacting port operations and border security. *See* 4-SER-849–62 (Ex. 89, Email Communications).

As explained by former Executive Director of Operations Vernon Foret, communications with Mexico concerning efforts to manage migration flows "should remain confidential, as disclosure to the public would stifle the free flow of information that is critical to maintaining a safe and secure border." *See* Foret Decl. ¶ 4. The information contained in this email chain provides "specific details" about law enforcement operations in the United States and Mexico, including "detailed operational data." Second Foret Decl. ¶ 7. "Officials on the ground must be able to communicate about all matters or issues that impact or have a potential impact to the border or border operations, without regard for the substance of the information shared or how it may be perceived by the public." *Id.* ¶ 5. Disclosure of these communications would chill the willingness of officials in the government of Mexico, or Mexico-based non-governmental organizations to share information with officials in CBP. Foret Decl. ¶¶ 5-6; Second Foret Decl. ¶ 8. As the district court recognized, the United States and the Government of Mexico's shared interest in maintaining confidentiality over communications "concerning migration efforts" provides a compelling reason to seal this information. *Al Otro Lado v. Wolf*, 2020 WL 4551687, at *6 (S.D. Cal. Aug. 6, 2020).

Law Enforcement Procedures. The Court should also continue the seal on information about particular law enforcement techniques that would enable individual travelers to try to evade those techniques, contained in 3-SER-600–38 (Ex. 8, OPR Investigation). *See* Declaration of Joseph Draganac ¶ 12 (attached as Exhibit E); *see also*, *e.g.*, *Hamdan v. U.S. Dep't of Justice*, 797 F.3d 759, 777–78 (9th Cir. 2015). Specifically, the Court should continue the seal on an internal instructional document for CBP Officers (at 3-SER-634) that does not relate to the issues in this case, and that contains instructions for vetting potential security threats at the border. *See Al Otro Lado, Inc. v. Wolf*, 2020 WL 4551687, at *11 (S.D. Cal. Aug. 6, 2020).

The security considerations raised by the operational information that the government is seeking to seal are like those raised in *United States ex rel. Kelly v. Serco, Inc.*, No. 11-cv-2975, 2014 WL 12675246, at *2 (S.D. Cal. Dec. 22, 2014), where the documents "specifically reference[d] locations, technical specifications and operational capabilities of restricted Homeland Security microwave communications systems along the United States border, used to provide technological assistance to federal agents tasked with monitoring and securing the border." The district court in that case concluded that "national security interests are a compelling reason for filing documents under seal[]" and because "the[] exhibits [at issue] contained sensitive technical information, such as specific tower locations and frequencies ... public dissemination of this information could be used by persons

seeking to do harm to the United States." According to the court, "[that] compelling reason outweighs the traditional right of access." *Id*. So too here, the information that the government seeks to seal would reveal sensitive law enforcement information vital to the ports' security, and its revelation would constitute irreparable harm. *See Washington*, 318 F. Supp. 3d at 1261 (the state government proved irreparable injury by showing harm in disclosing technical data relating to reproducing weapons).

B. Compelling Reasons Favor Sealing the Portions of the SER That Reflect or Describe Internal Governmental Policy Deliberations Such as Non-Final Policy Recommendations.

The Court should also seal portions of the SER that reflect internal deliberations regarding governmental decisions, which are protected from disclosure under the deliberative process privilege. *See* 4-SER-821–23 (Ex. 54, Email Communications); 4-SER-898–902 (Ex. 109, Email Communications); 4-SER-903–906 (Ex. 110, Email Communications); 4-SER-907–12 (Ex. 111, Email Communications).

The Court should seal this information, because it recounts or reflects "advisory opinions, recommendations, and deliberations comprising part of the process by which government decisions and policies are formulated." *Oceana Inc. v. Ross*, 2018 WL 5276297, at *2 (C.D. Cal. Aug. 20, 2018) (citing *FTC v. Warner Comm'ns, Inc.*, 742 F.2d 1156, 1161 (9th Cir. 1984)). Material is deliberative if it "would expose an agency's decisionmaking process in such a way to discourage

candid discussion within the agency and thereby undermine the agency's ability to perform its function." *Carter v. U.S. Dep't of Commerce*, 307 F.3d 1084, 1089 (9th Cir. 2002). Ultimately, such information is protected from disclosure so as to "protect[] and encourage[] the agency's ability to have candid discussions." *California Native Plant Society*, 251 F.R.D. at 411. Each of the documents listed in this section contain information that is protected from disclosure under this rationale.

The district court recognized that the information contained in Exhibits 109-111 (4-SER-898–912) is deliberative in nature and covered by the deliberative process privilege and warrants some protection from disclosure. *See Al Otro v. Mayorkas*, No. 17-cv-2366, ECF No. 543, 2020 WL 5422784, at *4 (S.D. Cal. Sept. 10, 2020). These exhibits contain pre-decisional, deliberative discussions weighing and recommending potential policy options, and internal deliberations regarding governmental decisions which are protected from disclosure under the same rationale underlying the deliberative process privilege. Thus, this Court should continue the seal the portions of these documents that contain deliberative communications and information.

C. Compelling Privacy Concerns Favor Continuing the Seal on Employee Contact Information and Sensitive Witness Information.

The Court should also continue the seal on employee contact information, such as email addresses and telephone numbers of government employees, as well as the identifying information of employees occupying law-enforcement sensitive positions and whistleblowers and witnesses to OIG investigations, which are found in the

following documents in Volumes 3-4: *See* 3-SER-519–34 (Ex. 22, OIG Memorandum and Exhibits); 3-SER-535–50 (Ex. 38, Leutert Merits Expert Report); 3-SER-600–38 (Ex. 8, OPR Investigation); 4-SER-812–15 (Ex. 29, Email Communications); 4-SER-816–19 (Ex. 38, Email Communications); 4-SER-821–23 (Ex. 54, Email Communications); 4-SER-846–48 (Ex. 83, April 2018 Metering Memo); 4-SER-895–97 (Ex. 105, Email Communications); 4-SER-898–902 (Ex. 109, Email Communications); 4-SER-903–906 (Ex. 110, Email Communications); SER-907-12 (Ex. 111, Email Communications); 4-SER-913–16 (Ex. 112, Email Communications). This information has no bearing on the merits of this appeal, and its public disclosure could result in serious threats to employee and witness privacy as well as agency security.

As detailed in the February 11, 2020 Declaration of John Buckley, the Director of Security and Technology Division at CBP, attached hereto as Exhibit F, there are genuine security concerns regarding the disclosure of CBP employees' email addresses, including "significant cyber security threats to both the individual employee and CBP as a whole." Ex. 3 ¶¶ 3-5. Dissemination of "the email addresses of CBP employees . . . can create significant cyber security threats to both the individual employee and CBP as a whole." Ex. D ¶ 3. For example, "once an employee's email address is publicized, malicious actors can engage in social engineering to obtain confidential information from that employee" through the "use

of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes," such as through phishing or spear phishing. *Id.* ¶ 4. "[O]ther cyber security threats can occur once an employee's email address is released to the public," such as a denial of service (DoS) attack. *Id.* ¶ 5.a. "[A] DoS is a security event that happens when an attacker prevents legitimate users from accessing specific computer systems, devices, services or other IT resources[, t]he purpose of [which] is to flood servers, systems, or networks with traffic to overwhelm the victim's resources and make it difficult or impossible for legitimate users to access them." *Id.* Another security threat is doxing, which "occurs when a malicious actor publishes private personal information, usually for purposes of public humiliation, stalking, identity theft, or targeting an individual for harassment." *Id.* Another threat is swatting, "a harassment tactic in which a malicious actor deceives emergency services into sending police or emergency response teams to another person's address." *Id.* Another example of a security threat from publicized emails involves ransomware, which "is malicious software designed to block access to a computer system until a sum of money is paid." *Id.* ¶ 5.d. Finally, spamming, which occurs when "disruptive online messages are sent repeatedly[], can "hinder an agency's ability to communicate with its employees due to the volume of email traffic and strains on the agency's IT capacities." *Id.* ¶ 5.e.

These security threats are not hypothetical. "Cyber attacks against the U.S. are

on the rise." *Id.* ¶ 6. A GAO report determined "that between 2006 and 2015, cyber attacks involving systems supporting the federal government increased over 1,300% from 5,500 to over 77,000." *Id.*; *see* GAO-16-501, Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems (May 2016). In fact, "[t]he Office of Personnel Management discovered it was the victim of a cyber attack in April 2015." *Id.* ¶ 7. Consequently, "[h]ackers stole personal information belonging to 21.5 million federal employees and their families, friends, and former employers." *Id.* These hackers "were able to compromise the entire OPM network by exploiting the credentials of one single contractor." *Id.* ¶ 7. Thus, "[p]ublication of CBP employees' email addresses . . . poses a substantial risk to the safety and welfare of the individual employee and CBP." *Id.* ¶ 8.

Many of these same concerns articulated in the Buckley declaration with respect to email addresses apply with equal force to other employee contact information such as telephone or fax numbers. For example, malicious actors can use employee phone numbers as well as emails to engage in "social engineering," a form of deception "to manipulate individuals into divulging confidential or person information." *See id.* ¶ 4. Malicious actors can similarly engage in "doxing" by publishing employee telephone numbers, which can lead to harassment of employees. *See id.* ¶ 5(b).

Further, the Court should permit the sealing of identifying information of

subjects of and witnesses to law enforcement and internal investigations, such as the whistleblower and other witnesses to an OIG investigation. In addition to the reasons provided above for sealing CBP employees' addresses, case law supports sealing this information. The Special Master in *Hewlett-Packard Co. S'holder Derivative Litig.* recommended sealing similar whistleblower identifying information in a criminal investigation because "the case law is clear that, while public access to court records is important, some documents are not subject to the public right of access because they have traditionally been kept secret for important policy reasons." *In re Hewlett-Packard Co. S'holder Derivative Litig.,* No. 12-CV-6003, 2015 WL 8570883, at *6 (N.D. Cal. Nov. 18, 2015), *report and recommendation adopted*, No. 12-CV-6003- CRB, 2015 WL 8479543 (N.D. Cal. Dec. 10, 2015), *aff'd*, 716 F. App'x 603 (9th Cir. 2017) (internal citations omitted). The Special Master in *Hewlett-Packard* explained that important public policy considerations, such as preventing interference with an investigation, "by making the whistleblower a target of intimidation or harassment" was a "compelling reason[]" constituting "court files [] becom[ing] a vehicle for improper purposes." *Id.* (internal citations omitted). Similar public policy reasons support sealing identifying information regarding other witnesses to the whistleblower investigation, as well as witnesses to, and subjects of, other internal investigations. *See also Al Otro Lado*, 2020 WL 4551687, at *3, 12 (permitting redaction of whistleblower's and witnesses' identities).

For these reasons, the Court should continue the seal on the portions of SER Volumes 3-4 that contain employee contact information and identifying information of employees with sensitive positions and witnesses to investigations.

CONCLUSION

For these reasons, this Court should seal the portions of SER Volumes 3-4 (Dkt. No. 29) identified above and in the attached redacted version of these volumes.

DATED: March 14, 2023

Respectfully submitted,

BRIAN M BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

WILLIAM C. PEACHEY
Director

ALEXANDER J. HALASKA
Senior Litigation Counsel

/s/ Katherine J. Shinners
KATHERINE J. SHINNERS
Senior Litigation Counsel
U.S. Department of Justice Civil Division
Office of Immigration Litigation
District Court Section
Washington, D.C. 20044
Tel: (202) 598-8259
katherine.j.shinners@usdoj.gov

JASON WISECUP
Trial Attorney

Counsel for the Government

CERTIFICATE OF COMPLIANCE

I certify that this motion complies with the word count limitation contained in Circuit Rule 32-3, because it uses proportionally spaced font, and contains 4,133 words, as measured by the word-processing application used to draft the document, which, when divided by 280, does not exceed twenty (20), the page-limit for motions as set forth in Circuit Rule 27-1(1)(d).

DATED: March 14, 2023

s/ Katherine J. Shinners
KATHERINE J. SHINNERS
Senior Litigation Counsel
United States Department of Justice

Counsel for the Government